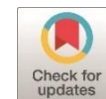


■ PRELIMINARY COMMUNICATION

Bihevioralni pristup upravljanju sigurnosnim rizicima: rezultati empirijskog istraživanja



Ivana Pokrajčić

"Dr. Franjo Tuđman" Defence and Security University, Zagreb, Croatia
ivana.pokrajcic@morh.hr  <https://orcid.org/0009-0001-2223-9122>

Submission: 2 July 2025 | Revision: 4 September 2025 | Acceptance: 18 September 2025

First published: 1 November 2025

<https://doi.org/10.22598/pi-be/2025.2.37620>

SAŽETAK

Svrha: U kontekstu rastućeg interesa za integraciju psiholoških i socijalnih dimenzija u upravljanje rizicima, cilj rada je analizirati međuodnos između bihevioralnih čimbenika i prihvaćenosti norme ISO 31000:2018. **Metodologija:** Teorijski okvir temelji se na teoriji planiranog ponašanja (TPB), uzimajući u obzir utjecaj stavova, subjektivnih normi i percipirane kontrole ponašanja na sigurnosno orijentirano ponašanje zaposlenika. Empirijsko istraživanje provedeno je na uzorku od 125 ispitanika, a analizirani su vanjski čimbenici (pritisak nadređenih, radna okolina) i unutarnji čimbenici (sigurnosna osviještenost, percipirana učinkovitost i izloženost rizicima) u odnosu na prihvaćenost norme. **Rezultati:** Istraživanje pokazuje statistički značajnu pozitivnu povezanost između utjecaja radne okoline i prihvaćenosti norme, dok je u slučaju pritiska nadređenih utvrđena negativna povezanost, što upućuje na otpor zaposlenika prema autoritarnom pristupu. Nalazi dodatno potvrđuju važnost sigurnosne kulture i pozitivne organizacijske klime u poticanju usklađenosti sa sigurnosnim normama. **Praktične implikacije:** Dobiveni rezultati pružaju empirijsku osnovu za redefiniranje organizacijskih strategija upravljanja rizicima kroz integraciju bihevioralnih uvida u institucionalne okvire, s ciljem povećanja učinkovitosti i održivosti sustava sigurnosnog upravljanja. **Originalnost/vrijednost:** Rad doprinosi literaturi empirijskim dokazima o ulozi bihevioralnih čimbenika u procesu prihvaćanja norme ISO 31000:2018, naglašavajući potrebu uključivanja psiholoških aspekata u razvoj organizacijske sigurnosne kulture i suvremenih praksi upravljanja rizicima.

Cljučne riječi: upravljanje rizicima, sigurnosni rizici, bihevioralna analiza, ISO 31000:2018

JEL codes: M14, L20, M10

Funding: The author declares no specific funding for this research.

Conflicts of Interest: The author declares no conflicts of interest.

The article is based on research conducted as part of the doctoral dissertation:

Pokrajčić, I. (2025). Determinants of the security risk management in middle and large companies in the segment of the national critical infrastructure of the Republic of Croatia in accordance to ISO 31000:2018. Doctoral dissertation.
<https://urn.nsk.hr/urn:nbn:hr:148:222681>

Data Availability Statement: The data that support the findings of this study are available from the author upon request.

Available online 1 November 2025

ISSN 1846-3355 / © 2025 The Author(s). Published by Poslovna izvrsnost - Business Excellence, University of Zagreb Faculty of Economics & Business.

This is an open access article under the terms of Creative Commons Attribution License [CC BY-NC 4.0](https://creativecommons.org/licenses/by-nc/4.0/).



1. Uvod

Upravljanje sigurnosnim rizicima predstavlja jedan od ključnih izazova suvremenih organizacija. Tradicionalni pristupi upravljanju rizicima uglavnom su usmjereni na tehničke i institucionalne aspekte, zanemarujući pritom značaj bihevioralnih čimbenika koji snažno utječu na efikasnost implementacije i poštivanja sigurnosnih politika i procedura. Međutim, u posljednjih nekoliko godina, posebice u okviru interdisciplinarnih istraživanja, prepoznaje se potreba integriranja psiholoških i socijalnih dimenzija u procese upravljanja rizicima, što predstavlja značajan iskorak u razumijevanju sigurnosno osviještenog ponašanja unutar organizacija (Scolobig i dr., 2015; Giovanetti, 2021).

Jedan od teorijskih okvira koji se ističe u proučavanju ljudskog ponašanja u organizacijama je Teorija planiranog ponašanja (engl. Theory of Planned Behavior - TPB) autora Ajzena (1991). Ova teorija pruža sustavan model kojim se mogu objasniti i predvidjeti namjere i ponašanja zaposlenika u vezi s pridržavanjem sigurnosnih standarda, s posebnim naglaskom na stavove, subjektivne norme te percepciju kontrole nad vlastitim ponašanjem. Empirijska istraživanja primjene TPB u kontekstu informacijskih i sigurnosnih politika ukazuju na značajan utjecaj individualnih uvjerenja, sigurnosne osviještenosti i organizacijskih očekivanja na ponašanje zaposlenika (Bulgurcu i dr., 2010; Merhi i dr., 2019; Herath i Rao, 2009a, 2009b).

ISO 31000:2018 je globalno priznati standard koji pruža smjernice za učinkovito upravljanje rizicima u organizacijama neovisno o njihovoj veličini ili djelatnosti. Standard opisuje strukturirani, fleksibilni i integrirani pristup koji obuhvaća prepoznavanje, analizu, upravljanje i praćenje rizika, s ciljem smanjenja štetnih utjecaja i iskorištavanja potencijalnih prilika za postizanje strateških ciljeva. Njegova važnost se očituje u naglasku na potrebu usklađivanja upravljanja rizicima s cjelokupnim strateškim usmjerenjem i okruženjem organizacije, uz uzimanje u obzir ljudskih i kulturnih čimbenika koji mogu značajno utjecati na uspješnost primjene (Pokrajčić i Lazibat, 2025). U kontekstu sigurnosnih rizika, primjena ove norme doprinosi standardizaciji procesa, transparentnosti i odgovornosti, integraciji tehničkih, institucionalnih ali i bihevioralnih aspekata upravljanja rizicima. Iako se u literaturi ponajprije ističe važnost institucionalnih mehanizama, poput sankcija i formalnih sigurnosnih politika, sve je jasnije da samo njihovo postojanje nije dovoljno za učinkovito upravljanje sigurnosnim rizicima. Ključni čimbenik uspjeha leži u razumijevanju bihevioralnih čimbenika koje potiču ili ograničavaju sigurnosno ponašanje zaposlenika. U tom kontekstu, normativni okvir ISO 31000:2018, koji definira temeljne principe upravljanja rizicima, pruža pogodno polazište za istraživanje integracije bihevioralnih i institucionalnih čimbenika u sustavni pristup upravljanju rizicima.

Cilj je rada kroz teorijski i empirijski pristup istražiti utjecaj vanjskih i unutarnjih bihevioralnih čimbenika u oblikovanju sigurnosnog ponašanja i prihvaćanja norme od strane zaposlenika, te time pridonijeti razvoju učinkovitijih strategija upravljanja sigurnosnim rizicima u složenim organizacijskim okruženjima.

2. Teorijski pregled dosadašnjih istraživanja kroz bihevioralni pristup

U cilju razumijevanja suvremenih pristupa upravljanju sigurnosnim rizicima, neophodno je sustavno analizirati postojeća istraživanja koja se bave institucionalnim i bihevioralnim aspektima ovog kompleksnog fenomena. Tijekom posljednja dva desetljeća sve je više radova koji upućuju na nužnost integracije tehničkih, organizacijskih i psiholoških dimenzija u oblikovanju učinkovitih sigurnosnih politika. U tom kontekstu, posebno je važna uloga doprinosa koji osvjetljavaju utjecaj organizacijske strukture, radnog okruženja, osobina ličnosti zaposlenika te percepcije rizika na razinu prihvaćenosti sigurnosnih normi i standarda.

Pritom se izdvajaju Scolobig i dr. (2015), koji među prvim naglašavaju važnost ljudski orijentirane perspektive u upravljanju rizicima, zagovarajući odmak od isključivo tehničkih

rješenja. Giovanetti (2021) dodatno razrađuje teorijske temelje za integraciju institucionalnih i bihevioralnih pristupa, dok Sommerstad i dr. (2016) empirijski potvrđuju složenost procesa prihvaćanja sigurnosnih standarda analizom 29 studija provedenih u poslovnim organizacijama. Značajan doprinos razumijevanju bihevioralnih čimbenika daju i Gratiana i dr. (2017), Pattinsona i dr. (2015) i Lounsburyja i dr. (2020), koji istražuju korelaciju između osobina ličnosti i poštivanja sigurnosnih procedura. Warrington (2021) unosi dodatnu vrijednost primjenom modela pet faktora ličnosti (engl. Five-Factor Model - FFM) i analizom razlika među generacijskim kohortama u pogledu sigurnosne svijesti. Teorijski okvir institucionalnog upravljanja sigurnošću temeljen na standardu ISO 31000:2018 razrađen je u člancima Lalondea (2012) i Olechowskog i dr. (2016), dok Boss i Kirsch (2007) ističu važnost formaliziranih sigurnosnih politika i hijerarhijskog pristupa implementaciji procedura.

S bihevioralne strane, autori poput Heratha i Rao (2009a, 2009b), Bulgurcua i dr. (2010), Taliba (2015) i Chongruia i dr. (2020) ukazuju na povezanost između motivacije zaposlenika, percepcije rizika i spremnosti na pridržavanje sigurnosnih pravila. Također, istraživanje AlKalbanija i dr. (2017) otvara važna pitanja o ulozi institucionalnog pritiska i organizacijske klime u oblikovanju sigurnosnog ponašanja.

Unatoč dosadašnjim doprinosima, u literaturi i dalje postoji manjak empirijskih analiza koje bi integrirale ove dvije razine - institucionalnu i bihevioralnu - u okviru konkretnih normativnih sustava poput ISO 31000:2018. Stoga se u ovom poglavlju daje sustavan pregled istraživanja s ciljem pronalaženja ključnih rezultata, identificiranja postojećih istraživačkih praznina i definiranja teorijskog okvira za daljnje ispitivanje odnosa između ponašanja zaposlenika i učinkovitosti institucionalnog upravljanja rizicima.

2.1. Bihevioralni pristup upravljanju rizicima

Unatoč sve većem broju radova o upravljanju rizicima, osobito onih koji pristupaju temi iz različitih teorijskih perspektiva, literatura koja ovu problematiku obrađuje iz bihevioralne dimenzije još je uvijek prilično oskudna. Većina postojećih istraživanja fokusira se na bihevioralne analize pojedinaca ili organizacijskih sustava, ispitujući sklonost rizičnom ponašanju i njegove uzročno-posljedične veze. Međutim, vrlo je mali broj istraživanja koje se bave analizom unutarnjih i vanjskih bihevioralnih čimbenika i njihovom povezanošću s institucionalnim dimenzijama upravljanja rizicima, kao što je standard ISO 31000:2018.

Tradicionalni institucionalni pristup polazi od pretpostavke da je cjelokupna odgovornost za upravljanje rizicima u nadležnosti organizacije, dok su zaposlenici u toj dinamici pasivni sudionici. U tom kontekstu, Boss i Kirsch (2007) naglašavaju kako je institucionalno nametanje obveze poštivanja sigurnosnih procedura - koje se u literaturi često označava kao implementacija sigurnosnih standarda i politika - proaktivan i široko prihvaćen pristup kojem bi sve organizacije trebale težiti. Suprotno njihovim tvrdnjama, Scolobig i dr. (2015) ističu kako je činjenica da je rani fokus istraživanja i primjene u području upravljanja rizicima bio primarno usmjeren na unapređenje tehnoloških kapaciteta i razvoj alata koji bi poduprli učinkovito upravljanje rizicima, te smatra kako je ovakav pristup proizlazio iz tadašnje pretpostavke da se problem rizika može najučinkovitije adresirati tehničkim i tehnološkim poboljšanjima te primjenom matematičkih prediktivnih modela. Definirali su institucionalno upravljanje rizicima kao hijerarhijski organiziran proces, u kojem se razina implementacije i koordinacije prilagođava veličini, opsegu i djelatnosti organizacije. Međutim, isti autori prepoznaju važnost ljudskog faktora, promovirajući tzv. „ljudski orijentiranu“ perspektivu (engl. people-centric perspective), te ističu kako za ostvarenje stvarne učinkovitosti i sinergije institucionalnog pristupa i ljudskog faktora u upravljanju rizicima nije dovoljno samo deklarirati participativne pristupe, već je potrebna njihova autentična integracija. U novijim radovima, autori poput Giovanettija (2021), Koohanga i dr. (2020), Kaymaza (2020) te Crama i Proudfoota (2014) dodatno se razvijaju teorijski pristupi koji

integriraju institucionalne i bihevioralne (unutarnje i vanjske) odrednice, naglašavajući njihov zajednički utjecaj na organizacijsku kulturu i učinkovitost upravljanja rizicima.

U relevantnoj literaturi se upravljanje rizicima promatra kao dinamičan i višedimenzionalan proces koji se kontinuirano razvija te uključuje integrirani pristup temeljen na kombinaciji tehničke ekspertize i razumijevanja društvenih, bihevioralnih, ekonomskih i institucionalnih čimbenika. Giovanetti (2021) navodi kako su potvrđeni učinci bihevioralnih čimbenika na učinkovitost sustava upravljanja rizicima, posebice u okviru institucionalnih okvira. Sommerstad i dr. (2016) su analizirali 29 empirijskih istraživanja koja su se bavila čimbenicima koji utječu na prihvaćanje i implementaciju sigurnosnih standarda i procedura u poslovnim organizacijama. Na temelju rezultata zaključili su kako su potrebna podrobnija istraživanja o utjecaju bihevioralnih čimbenika na pridržavanje sigurnosnih propisa i smanjenje sigurnosnih rizika u poslovnom kontekstu.

Empirijska istraživanja autora kao što su Gratian i dr. (2017), Pattinson i dr. (2015) te Lounsbury i dr. (2020) pokazala su postojanje korelacije između specifičnog skupa osobina ličnosti i ponašanja zaposlenika u području informacijske sigurnosti. Warrington (2021) otišao je korak dalje istražujući povezanost generacijskih kohorti sa sigurnosnom sviješću i pridržavanjem sigurnosnih procedura, pritom primjenjujući bihevioralni model pet faktora ličnosti. Gratian i dr. (2017) dokazali su da osobine poput ličnosti, sklonosti financijskom riziku, ekstroverzije, racionalnog donošenja odluka i spola statistički značajno utječu na ponašanje zaposlenika u odnosu na propisane sigurnosne procedure u kontekstu kibernetičke sigurnosti. Slične rezultate donose i Pattinson i dr. (2015), koji su pokazali da faktori poput dobi, razine obrazovanja, sposobnosti kontrole impulzivnosti, računalne pismenosti i osobnosti značajno koreliraju s poštivanjem sigurnosnih propisa.

Kroz godine, brojni su istraživači pokušali dublje razumjeti bihevioralne čimbenike koji motiviraju zaposlenike da se pridržavaju sigurnosnih pravila. Generalni zaključak tih istraživanja jest da ključnu ulogu imaju vanjski (Straub, 1990; Bulgurcu i dr., 2010; Herath i Rao, 2009a, Herath i Rao, 2009b) i unutarnji čimbenici (Herath i Rao, 2009a). Vanjski bihevioralni čimbenici uključuju čimbenike poput pritiska nadređenih (Herath i Rao, 2009a; Bulgurcu i dr., 2010), sustava nagrađivanja (Boss i dr., 2009), utjecaja radnog okruženja (Herath i Rao, 2009a; Talib, 2015) te organizacijske klime. U tom kontekstu, Herath i Rao (2009b) istražili su odnos između radnog okruženja i namjere zaposlenika da poštuju sigurnosne procedure, te su utvrdili snažnu pozitivnu korelaciju između tih varijabli ($r = .91$). Nadalje, isti autori su utvrdili kako postoji vrlo niska korelacija između pritiska nadređenih, uključujući i sankcioniranje zaposlenika, i namjere zaposlenika da poštuju propisane sigurnosne norme ($r = .13$), te je utvrđena i iznimno niska korelacija između pritiska nadređenih i organizacijske odanosti ($r = .11$) (Herath i Rao, 2009b). Suprotno ostvarenim rezultatima od Herath i Rao (2009b), AlKalbani i dr. (2017) su u dokazali da institucionalni pritisci imaju snažan pozitivan utjecaj na pridržavanje sigurnosnih procedura ($r = .76$). Treba napomenuti da je njihov rad bilo primarno usmjereno na ispitivanje utjecaja zakonske regulative i drugih normativnih akata na ponašanje menadžmenta, odnosno na njihovu spremnost za implementaciju sigurnosnih politika unutar organizacijskog sustava. Nadalje, AlKalbani i dr. (2017) u okviru istraživanja poštivanja sigurnosnih procedura u području informacijske sigurnosti pretpostavili su da utjecaj radnog okruženja pozitivno utječe na ponašanje zaposlenika, što je empirijski i potvrđeno. Njihovo istraživanje pokazalo je značajnu pozitivnu korelaciju ($r = .61$) između karakteristika radnog okruženja i sklonosti zaposlenika da se pridržavaju propisanih sigurnosnih procedura, i u skladu je s rezultatima istraživanja Herath i Rao (2009a; 2009b). Unutarnji bihevioralni čimbenici se odnose na individualnu percepciju, motivaciju i stavove samih zaposlenika. Herath i Rao (2009a) naglašavaju da unutarnja motivacija ima značajan utjecaj na ponašanje zaposlenika, osobito u kontekstu prihvaćanja propisanih sigurnosnih normi i procedura. Talib (2015) dodatno tvrdi da unutarnji bihevioralni čimbenici imaju snažniji pozitivan učinak na prihvaćanje sigurnosnih mjera u odnosu na vanjske. Do sličnih rezultata došli su i Chongruija i dr. (2020) jer su potvrdili

postojanje povezanosti između percipirane učinkovitosti i izloženosti organizacije sigurnosnim rizicima te poštivanja propisanih sigurnosnih normi od strane zaposlenika. Iako su neka istraživanja ispitivala utjecaj unutarnjih bihevioralnih čimbenika kao što su sigurnosne osviještenosti, percipirane učinkovitosti upravljanja rizicima i percipirane izloženosti organizacije rizicima; na sigurnosno ponašanje zaposlenika, dosad nije provedeno empirijsko istraživanje koje bi ispitalo utječu li ti čimbenici na prihvaćenost načela norme ISO 31000:2018. Herath i Rao (2009b) su, na teorijskoj razini, istraživali ponašanje zaposlenika u odnosu na njihovu namjeru usklađenosti sa sigurnosnim politikama, koristeći integrirani okvir koji obuhvaća teoriju motivacije za zaštitu, teoriju odvracanja, teoriju organizacijske predanosti i teoriju planiranog ponašanja. Rezultati istraživanja otkrivaju kako zaposlenici koji ozbiljno percipiraju rizike i imaju visoku razinu sigurnosne svijesti znatno dosljednije usklađuju svoje ponašanje s propisanim sigurnosnim procedurama ($r = .76$). Slične rezultate daje i istraživanje od Bulgurcu i dr. (2010), koje potvrđuje postojanje pozitivne korelacije između razine sigurnosne osviještenosti zaposlenika i njihove namjere da se pridržavaju propisanih sigurnosnih pravila ($r = 0,59$). Nadalje, dosadašnja istraživanja pokazuju da će zaposlenici razviti negativan stav prema sigurnosnim procedurama ako ih percipiraju kao neučinkovite ili kao prepreku svakodnevnom obavljanju posla (Herath i Rao, 2009b). Ovi autori ističu kako je od iznimne važnosti da rukovoditelji prenesu zaposlenicima (ali i krajnjim korisnicima) realnu sliku o prijetnjama sigurnosti, kako bi se kod njih razvila „percepcija izloženosti“, što je ključni element za aktiviranje zaštitnog ponašanja. Iz navedenog proizlazi da je odgovornost menadžmenta ne samo implementirati sigurnosne standarde, već i učinkovito komunicirati njihovu važnost, ističući kako su pridržavanje pravila i ponašanje zaposlenika ključni za postizanje sveukupne sigurnosti poslovanja, što je u skladu sa poimanjem ranije spomenute autentične integracije na koju pozivaju Scolobig i dr. (2015). Analizirana istraživanja potvrđuju da bihevioralni vanjski i bihevioralni unutarnji čimbenici mogu utjecati na ponašanje zaposlenika i njihovu sklonost prihvaćanju institucionalnih sigurnosnih normi, dio literature dovodi u pitanje postojanje dosljedne korelacije pozivajući se na Siponen i Vance (2010) koji smatraju da određeni dio ispitanika subjektivno pristupa istraživanjima, pri čemu dolazi do racionalizacije ili neutralizacije vlastitih stavova, što otežava interpretaciju nalaza. Predmet ovog rada je utjecaj vanjskih i unutarnjih bihevioralnih čimbenika na prihvaćenost norme ISO 31000:2018. U Tablici 1 prikazana su relevantna istraživanja korištena pri oblikovanju varijabli empirijskog istraživanja.

Tablica 1.

Prikaz odabranih dosadašnjih istraživanja bihevioralnih čimbenika

Varijabla	Dosadašnja istraživanja
Bihevioralni vanjski čimbenik	Straub (1990) Herath i Rao (2009a; 2009b) Bulgurcu i dr. (2010) Talib (2015)
Bihevioralni unutarnji čimbenik	Herath i Rao (2009a; 2009b) Bulgurcu i dr. (2010) Siponen i dr. (2014) Chongrui i dr. (2020)

Izvor: autor.

2.2. Teorija planiranog ponašanja

Teorija planiranog ponašanja koju je razvio Ajzen (1991) predstavlja jednu od najutjecajnijih teorijskih osnova za predviđanje i razumijevanje ljudskog ponašanja u specifičnim

kontekstima. Temeljna pretpostavka ove teorije jest da je ponašanje pojedinca rezultat njegove namjere da ga provede, a ta je namjera oblikovana trima ključnim čimbenicima: stavovima, subjektivnim normama i percipiranom kontrolom ponašanja. Stavovi predstavljaju opću evaluaciju pojedinca o ciljanom ponašanju, utemeljenu na njegovim uvjerenjima o ishodima tog ponašanja i vrijednosti koju pridaje tim ishodima. Pozitivni stavovi povećavaju vjerojatnost formiranja namjere da se određeno ponašanje provede. Subjektivne norme odnose se na percipirani društveni pritisak, odnosno uvjerenja pojedinca o tome što važni referentni akteri, kao što su kolege, nadređeni ili bliske osobe - očekuju od zaposlenika u vezi s ponašanjem, kao i na njegovu motivaciju da se tim očekivanjima prilagodi. Percipirana kontrola ponašanja označava procjenu pojedinca o lakoći ili težini provedbe određenog ponašanja, pri čemu važnu ulogu imaju unutarnji i vanjski čimbenici koji mogu olakšati ili otežati ostvarenje ponašajnih namjera. Sukladno ovoj teoriji, što su stavovi pojedinca pozitivniji, subjektivne norme snažnije, a percipirana kontrola ponašanja veća, to je vjerojatnije da će se razviti snažna namjera za provedbu ponašanja, a posljedično i samo ponašanje.

U empirijskom istraživanju koje su proveli Bulgurcu i dr. (2010), a koje je bilo utemeljeno upravo na teoriji planiranog ponašanja, analizirani su organizacijski čimbenici koji utječu na ponašanje zaposlenika u odnosu na pridržavanje sigurnosnih politika. Rezultati su pokazali da je namjera zaposlenika da se pridržavaju sigurnosnih pravila značajno uvjetovana njihovim osobnim stavovima, normativnim uvjerenjima i razinom sigurnosne osviještenosti. Posebno je naglašena uloga uvjerenja zaposlenika da njihovo ponašanje ima pozitivan utjecaj na ukupnu sigurnost organizacije, što se često prenosi i na kolege putem organizacijske socijalizacije (Bulgurcu i dr., 2010). Također je utvrđeno da sigurnosna osviještenost pozitivno utječe na oblikovanje stavova i uvjerenja o poželjnim ishodima ponašanja. Nadalje, Merhi i dr. (2019) analizirali su ulogu sankcija kao organizacijskog mehanizma u oblikovanju kognitivnih uvjerenja zaposlenika o sigurnosnim politikama i njihovoj namjeri pridržavanja istih. Autori su operacionalizirali institucionalno kažnjavanje kroz dva aspekta: percipiranu sigurnost sankcioniranja (odnosno vjerojatnost otkrivanja i sankcioniranja nepoželjnih ponašanja) te percipiranu ozbiljnost kazne (odnosno intenzitet predviđenih sankcija). Iako su rezultati bili djelomično mješoviti, općenito je potvrđeno da percepcija kazne kao ozbiljne, u kombinaciji s visokom percepcijom detekcije devijantnog ponašanja, djeluje odvraćajuće na nepoštivanje sigurnosnih politika. Prema autorima, organizacijska kazna može oblikovati kognitivne procese zaposlenika tako što internaliziraju strah od posljedica, što posljedično vodi većoj posvećenosti poštivanju sigurnosnih pravila (Merhi i dr., 2019). Takvi mehanizmi mogu također utjecati na subjektivne norme, jer kroz formalne politike i sankcije organizacija komunicira jasna očekivanja prema zaposlenicima. U skladu s navedenim, Blythe i dr. (2015) empirijski su potvrdili da su ponašanja zaposlenika u kontekstu pridržavanja sigurnosnih procedura značajno oblikovana njihovim sigurnosnim znanjem i prethodnim iskustvom, čime se dodatno naglašava važnost obrazovanja i obuke kao sastavnica sigurnosne kulture. Herath i Rao (2009a) su, nadograđujući se na teoriju planiranog ponašanja koristili i teoriju odvrćanja i teoriju motivacije za zaštitu kako bi dodatno objasnili motivacijske čimbenike ponašanja zaposlenika prema organizacijskim sigurnosnim politikama. Njihovo istraživanje ukazalo je na važnost bilateralnog odnosa između organizacije i zaposlenika, posebno u pogledu percepcije pravednosti i legitimnosti sigurnosnih procedura, što izravno utječe na razinu pridržavanja. Iako su njihova istraživanja bila primarno usmjerena na područje informacijske sigurnosti, njihovi zaključci su primjenjivi i na širi kontekst upravljanja organizacijskim rizicima.

Teorija planiranog ponašanja pruža snažan teorijski okvir za razumijevanje i predviđanje ponašanja zaposlenika u kontekstu organizacijskog pridržavanja sigurnosnih politika i procedura. Istraživanja koja su primjenjivala ovaj model u području informacijske i organizacijske sigurnosti jasno upućuju na to da su stavovi, subjektivne norme i percipirana kontrola ponašanja ključni prediktori namjere zaposlenika da se ponašaju u skladu s propisanim standardima. Posebnu važnost pritom imaju individualna uvjerenja zaposlenika o

učinkovitosti sigurnosnih mjera, percepcija organizacijskih očekivanja, kao i doživljaj osobne odgovornosti i kontrole. Dodatno, institucionalni mehanizmi poput sustava sankcija i formalnih politika mogu utjecati na kognitivne procese zaposlenika, oblikujući njihovu percepciju o posljedicama devijantnog ponašanja i time jačajući usklađenost s pravilima.

3. Hipoteze i metodologija

3.1. Razvoj hipoteza

Temeljem rezultata istraživanja ([Pokrajčić, 2025](#)) koji se odnose na prihvaćenost temeljnih odrednica norme ISO 31000:2018 i temeljem ranijih dosadašnji istraživanja bihevioralnih čimbenika i njihovog utjecaja na sigurnosno osviješteno ponašanje zaposlenika te na upravljanje rizicima, glavna istraživačka pitanja (IP) koja su temelj za postavljanje hipoteza i provedbu istraživanja glase:

IP₁: Utječu li i u kojoj mjeri vanjski bihevioralni čimbenici na sigurnosno osviješteno ponašanje zaposlenika?

IP₂: Utječu li i u kojoj mjeri unutarnji bihevioralni čimbenici na sigurnosno osviješteno ponašanje zaposlenika?

IP₃: Utječu li i u kojoj mjeri bihevioralni čimbenici na prihvaćenost norme ISO 31000:2018?

U radu se postavljaju dvije glavne hipoteze i pod hipoteze proizašle iz teorijskog okvira utemeljenog na teoriji planiranog ponašanja. Pomoću njih će se otkriti način na koji bihevioralni i organizacijski čimbenici utječu na usvajanje sigurnosnih standarda u praksi upravljanja rizicima.

Poticažno radno okruženje - koje karakteriziraju otvorena komunikacija, podržavajuće vodstvo i razvijena sigurnosna kultura - olakšava internalizaciju sigurnosnih normi među zaposlenicima. Prva hipoteza treba potvrditi koncept organizacijske klime kao ključnog prediktora sigurnosnog ponašanja, čime se otvara prostor za oblikovanje učinkovitijih strategija upravljanja ljudskim faktorom u ovakvim organizacijama. Hipoteza i podhipoteze glase:

H₁: Vanjski bihevioralni čimbenici imaju statistički značajan i pozitivan utjecaj na prihvaćenost norme ISO 31000:2018.

H_{1a}: Radna okolina pozitivno utječe na prihvaćanje norme ISO 31000:2018.

H_{1b}: Pritisak nadređenih korelira negativno s prihvaćanjem norme ISO 31000:2018.

Strogi autoritativni pristup i metode provedbe sigurnosnih procedura mogu izazvati otpor zaposlenika te smanjiti njihovu unutarnju motivaciju za poštivanje sigurnosnih standarda. Potrebno je dokazati negativne posljedice pritiska nadređenih i njihovih hijerarhijski dominantnih pristupa, čime bi se naglasila potreba za participativnim modelima upravljanja i razvojem sigurnosnog vodstva temeljenog na povjerenju i kompetencijama, a ne na kontroli. Prema tome, postavlja se slijedeća hipoteza i podhipoteze:

H₂: Bihevioralni unutarnji čimbenici imaju statistički značajan utjecaj na prihvaćenost norme ISO 31000:2018.

H_{2a}: Sigurnosna osviještenost pozitivno utječe na prihvaćanje norme ISO 31000:2018.

H_{2b}: Percipirana učinkovitost pozitivno doprinosi prihvaćanju ISO 31000:2018.

H_{2c}: Percipirana izloženost pozitivno utječe na prihvaćanje norme ISO 31000:2018.

3.2. Metodologija

U svrhu istraživanja proveden je anketni upitnik na uzorku od ukupno 125 ispitanika zaposlenih u srednjim i velikim poduzećima sa sjedištem u Hrvatskoj. Svi ispitanici obavljaju poslove koji su izravno povezani s upravljanjem sigurnosnim rizicima, čime se osigurava relevantnost dobivenih podataka u odnosu na istraživački fokus. Raspodjela sudionika prema veličini organizacije u kojoj su zaposleni prikazana je u [Tablici 2](#). Veći udio ispitanika

dolazi iz velikih poduzeća (N=70), dok je iz srednjih poduzeća sudjelovalo 53 ispitanika. Dvoje sudionika nije moglo precizno odrediti veličinu organizacije u kojoj su zaposleni, stoga su njihovi odgovori isključeni iz analize razlika između srednjih i velikih poduzeća.

Tablica 2.

Raspodjela sudionika s obzirom na veličinu poduzeća.

Tip poduzeća prema broju zaposlenika	<i>n</i>	%
Srednje (> 50, < 250)	53	42.4
Veliko (> 250)	70	56.0
Ne znam	2	1.6

Izvor: autor prema statističkoj kategorizaciji Eurostata, dostupno na: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Enterprise_size

Ispitanici su preko Likertove skale dali svoje odgovore na pojedinačne tvrdnje, te se zbirna varijabla o bihevioralnim unutarnjim odrednicama formirala kao aritmetička sredina skupine pitanja o bihevioralnim unutarnjim odrednicama triju podhipoteza i testirala korištenjem Cronbach alpha koeficijenta. Za potrebe istraživanja u svrhu testiranja postavljenih hipoteza kao istraživački instrument ispitanicima je putem online platforme distribuiran anketni upitnik. Upitnik se sastojao od skupa tvrdnji (Tablica 3.) koje su ispitanicima omogućile izražavanje stupnja slaganja na Likertovoj skali od pet stupnjeva. Prvi dio istraživačkog instrumenta mjerio je prihvaćenost norme ISO 31000:2018. Drugi dio fokusirao se na mjerenje bihevioralnih unutarnjih čimbenika, konkretno sigurnosne svjesnosti ispitanika, njihove percepcije učinkovitosti procesa upravljanja sigurnosnim rizicima, kao i percipirane izloženosti poduzeća sigurnosnim rizicima. Treći dio obuhvaćao je mjerenje bihevioralnih unutarnjih čimbenika, koja uključuje vanjske čimbenike (pritisak nadređenih i utjecaj radne okoline), a koji djeluju na zaposlenike te utječu na njihovu spremnost na prihvaćanje normi i procesa upravljanja sigurnosnim rizicima.

Tablica 3.

Prikaz varijabli i načina njihovog mjerenja.

Bihevioralni unutarnji čimbenici	Anketno pitanje
Sigurnosna svjesnost	Q1. Redovno sudjelujem na edukacijama iz područja sigurnosti
	Q2. Upoznat sam sa svim zakonskim i podzakonskim propisima iz područja sigurnosti
	Q3. Ako poštujemo propisane sigurnosne procedure, moje poduzeće će bolje poslovati
	Q4. Jasna mi je potreba poštivanja sigurnosnih procedura na individualnoj i organizacijskoj razini
	Q5. Jasna mi je potreba upravljanja sigurnosnim rizicima na organizacijskog razini
Percipiranost učinkovitosti	Q6. Svjestan/svjesna sam potencijalnih sigurnosnih rizika u mom poduzeću
	Q7. Svaki zaposlenik mog poduzeća može doprinijeti sprječavanju nastanka sigurnosnog incidenta
	Q8. Mjere iz područja sigurnosti koje se provode u mom poduzeću su učinkovite
	Q9. Upravljanje sigurnosnim rizicima je dobro za poduzeće

Percipiranost izloženosti	Q10. Moje poduzeće izloženo je riziku od krađe intelektualnog vlasništva Q11. Moje poduzeće izloženo je riziku od krađe osobnih podataka zaposlenika, klijenata i partnera Q12. Moje poduzeće izloženo je riziku od narušavanja poslovnih procesa Q13. Moje poduzeće izloženo je riziku od krađe materijalnih sredstava i imovine Q14. Zaposlenici u mom poduzeću izloženi su sigurnosnom riziku. Q15. Izloženost sigurnosnim rizicima može značajno naštetiti poslovanju mog poduzeća
Bihevioralni vanjski čimbenici	
Pritisak nadležnih	Q16. Upravljanje sigurnosnim rizicima nepotrebno je nametnuto poduzeću od strane nadležnih osoba, institucija ili države Q17. Moja odgovornost prema nadležnima u području upravljanja sigurnosnim rizicima je velika. Q18. Sa razine nadležnih osoba i institucija provodi se redovan nadzor implementacije i poštivanja propisa iz područja upravljanja sigurnosnim rizicima Q19. Nepoštivanje propisa može imati negativne posljedice za mene i poduzeće
Utjecaj radne okoline	Q20. Moji kolege, suradnici i partneri razumiju i poštuju sve propisane sigurnosne procedure Q21. Većina zaposlenika u mom poduzeću poštuje sve propisane sigurnosne procedure Q22. Zaposlenici u mom poduzeću imaju pozitivan stav prema propisanim sigurnosnim procedurama. Q23. Konkurentska poduzeća su implementirala sve propise iz područja upravljanja sigurnosnim rizicima

Izvor: autor.

Za deskriptivnu analizu prikupljenih podataka korištena je aritmetička sredina i standardna devijacija. Distribucije su dodatno analizirane određivanjem minimalnih i maksimalnih vrijednosti, kao i koeficijenta asimetrije i vršnosti. Normalnost distribucija testirana je Kolmogorov-Smirnov testom. U kontekstu institucionalnih odrednica norme ISO 31000:2018, kao i bihevioralnih vanjskih i unutarnjih čimbenika, faktorska struktura korištenih ljestvica ispitana je analizom glavnih komponenti, budući da su ljestvice konstruirane posebno za potrebe ovog istraživanja. Prije provođenja faktorske analize, međusobne povezanosti između varijabli uključenih u analizu određene su pomoću Pearsonova koeficijenta korelacije. Za identifikaciju broja dimenzija koje se nalaze u osnovi mjerenih varijabli primijenjen je Kaiser-Guttmanov kriterij, koji odabire dimenzije sa svojstvenom vrijednošću većom od jedan. Dodatno je korišten i Scree-test, temeljen na kriteriju značajnijeg pada u vrijednostima svojstvenih vrijednosti. Ukupni rezultati na korištenim ljestvicama izračunati su kao aritmetička sredina odgovora na pojedine stavke ljestvice, dok je pouzdanost ljestvica procijenjena Cronbachovim alfa koeficijentom unutarnje konzistencije.

4. Rezultati istraživanja i interpretacija

4.1. Deskriptivna analiza podataka

Aritmetičke sredine (M) i standardne devijacije (SD) čestica korištenih za ispitivanje prihvaćenosti norme ISO 31000:2018, kao i vanjskih i unutarnjih bihevioralnih čimbenika, prikazane su u [Tablici 4](#). U segmentu koji se odnosi na vanjske bihevioralne čimbenike, a

posebno na pritisak nadređenih, jedna čestica procjenjuje upravljanje sigurnosnim rizicima kao posljedicu izravnog utjecaja nadređenih. Preostale tri čestice, koje se odnose na samoinicijativno i odgovorno ponašanje zaposlenika bile su usmjerene na procjenu upravljanja sigurnosnim rizicima temeljenog na osobnoj odgovornosti i unutarnjoj motivaciji zaposlenika, te su stoga interpretacijski suprotne navedenoj dimenziji i analizirane su kao obrnuto bodovane varijable. Podaci sugeriraju da su sigurnosna svjesnost i percepcija učinkovitosti upravljanja rizicima najizraženije dimenzije u organizaciji, dok postoji prostor za jačanje institucionalnih pritisaka, prihvatanja standarda i utjecaja radne okoline na sigurnosno ponašanje. Ove informacije mogu poslužiti kao smjernice za usmjeravanje budućih intervencija i politika u cilju unaprjeđenja cjelokupnog sustava upravljanja sigurnošću.

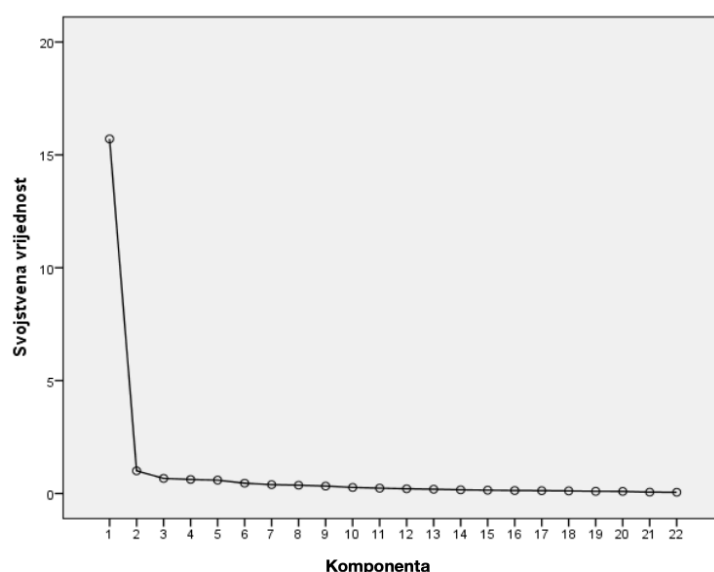
Tablica 4.

Aritmetičke sredine i standardne devijacije varijabli.

Varijabla	M	SD
(ISO) Prihvaćenost ISO 31000:2018	3.72	1.25
(BVČ) Bihevioralni vanjski čimbenici	3.53	1.25
(PN) Pritisak nadležnih	3.68	1.29
(URO) Utjecaj radne okoline	3.39	1.22
(BUČ) Bihevioralni unutarnji čimbenici	3.99	1.02
(SS) Sigurnosna svjesnost	4.02	0.89
(PU) Percipiranost učinkovitosti	4.36	0.78
(PI) Percipiranost izloženosti	3.59	1.30

Izvor: autor.

Analiza glavnih komponenata, kao što je prikazano na [Slici 1.](#), provedena je na skupu svih čestica konstruiranih za mjerenje prihvaćenosti norme ISO 31000:2018. Rezultati analize pokazali su da se, prema Kaiser-Guttmanovu kriteriju, u osnovi odgovora ispitanika mogu izdvojiti dvije latentne dimenzije, s obzirom na to da su dvije komponente imale svojstvenu vrijednost veću od jedan. Ipak, prva komponenta imala je znatno veću svojstvenu vrijednost u odnosu na drugu, što sugerira postojanje dominantne latentne dimenzije. Ta dimenzija objašnjava 71.40 % ukupne varijance varijabli uključenih u analizu, što upućuje na visoku unutarnju povezanost čestica i opravdava njihovo objedinjavanje u jedinstvenu mjeru prihvaćenosti norme.



Slika 1.

Svojstvene vrijednosti svih glavnih komponenata u pozadini čestica namijenjenih mjerenju prihvaćenosti norme ISO 31000:2018.

Izvor: autor.

4.2. Analiza čestica namijenjenih mjerenju bihevioralnog unutarnjeg čimbenika

Deskriptivna statistika čestica namijenjenih mjerenju sigurnosne svjesnosti zaposlenika prikazana je u [Tablici 5](#). Rezultati pokazuju da ispitanici imaju visoku razinu svjesnosti o važnosti sigurnosnih procedura i upravljanja sigurnosnim rizicima, iako je njihovo redovno sudjelovanje na edukacijama o sigurnosti nešto niže ocijenjeno. Izjava „Redovno sudjelujem na edukacijama iz područja sigurnosti” dobila je relativno nisku prosječnu ocjenu ($M = 2.65$; $SD = 1.53$), što upućuje na to da velik broj ispitanika ne sudjeluje često u sigurnosnim edukacijama ili da se to ne prakticira redovito u njihovim poduzećima. Ispitanici su pak izrazili da su dobro upoznati sa zakonskim i podzakonskim propisima iz područja sigurnosti ($M = 3.77$; $SD = 1.25$), što pokazuje umjereno do visoko znanje o relevantnim propisima. Visoke srednje vrijednosti na izjavama poput „Ako poštujemo propisane sigurnosne procedure, moje poduzeće će bolje poslovati” ($M = 4.22$; $SD = 0.81$), „Jasna mi je potreba poštivanja sigurnosnih procedura na individualnoj i organizacijskoj razini” ($M = 4.69$; $SD = 0.47$) te „Jasna mi je potreba upravljanja sigurnosnim rizicima na organizacijskoj razini” ($M = 4.78$; $SD = 0.41$) ukazuju na snažno prihvaćanje važnosti sigurnosnih mjera i svijest o njihovoj važnosti za poslovanje i organizacijsku funkciju. Rezultati Kolmogorov-Smirnov testa za sve čestice pokazuju statistički značajna odstupanja od normalne raspodjele ($p < 0.001$), što upućuje na asimetričnu distribuciju odgovora, često s naglaskom na visoke ocjene kod većine sudionika. Može se zaključiti kako ispitanici jasno prepoznaju važnost sigurnosnih procedura i upravljanja rizicima na individualnoj i organizacijskoj razini, što upućuje na visoku sigurnosnu svjesnost. Međutim, manji odaziv na redovne edukacije sugerira prostor za unaprijeđenje u području kontinuiranog obrazovanja i podizanja sigurnosne kulture kroz obuke.

Tablica 5.*Sigurnosna svjesnost.*

Čestica	min	max	M	SD	K-S test	
					z	p
Q1	1	5	2.65	1.53	0.23	< .001
Q2	1	5	3.77	1.25	0.29	< .001
Q3	2	5	4.22	0.81	0.28	< .001
Q4	4	5	4.69	0.47	0.44	< .001
Q5	4	5	4.78	0.41	0.48	< .001

Izvor: autor.

Rezultati mjerenja percipiranosti učinkovitosti pokazuju da ispitanici u velikoj mjeri percipiraju da su sigurnosni rizici u njihovim poduzećima jasno prepoznati te da se upravljanje tim rizicima smatra učinkovitom praksom. Svi odgovori statistički su značajno odstupali od normalne raspodjele ($p < .001$ prema K-S testu), što znači da su distribucije rezultata asimetrične, s većinom ispitanika koji daju visoke ocjene (Tablica 6.) To je bilo osobito vidljivo kod čestica Q6 i Q9 na koje su ispitanici u velikom broju odgovarali najvišim ocjenama na ponuđenoj ljestvici, a kojima ispitanici izražavaju visok stupanj vlastite svjesnosti o potencijalnim sigurnosnim rizicima koji mogu naštetiti njihovim poduzećima, odnosno o vlastitoj ulozi u sprječavanju nastanka istih. Ukupno gledano, ispitanici pokazuju visok stupanj svijesti o sigurnosnim rizicima i smatraju da je upravljanje tim rizicima učinkovito i korisno za poduzeće. Međutim, raznolikost u procjeni učinkovitosti konkretnih mjera upućuje na potencijalni prostor za dodatna poboljšanja i komunikaciju oko sigurnosnih praksi unutar organizacije.

Tablica 6.*Percipiranost učinkovitosti.*

Čestica	min	max	M	SD	K-S test	
					z	p
Q6	4	5	4.66	0.48	0.42	< .001
Q7	2	5	4.26	0.88	0.27	< .001
Q8	1	5	3.78	1.32	0.25	< .001
Q9	4	5	4.74	0.44	0.46	< .001

Izvor: autor.

Rezultati mjerenja percipiranosti izloženosti sigurnosnim rizicima (Tablica 7.) upućuju na to da ispitanici percipiraju kako su njihova poduzeća najranjivija na rizike povezane s krađom osobnih podataka zaposlenika, klijenata i poslovnih partnera, kao i na krađu materijalne imovine. S druge strane, najmanje vjeruju da su sami zaposlenici izravno izloženi sigurnosnim rizicima.

Tablica 7.*Percipiranost izloženosti.*

Čestica	min	max	M	SD	K-S test	
					z	p
Q10	1	5	2.51	1.53	0.26	< .001
Q11	1	5	3.76	1.45	0.29	< .001
Q12	1	5	4.51	1.01	0.42	< .001
Q13	1	5	3.74	1.44	0.29	< .001
Q14	1	5	2.87	1.43	0.24	< .001
Q15	1	5	4.17	0.93	0.25	< 0.001

Izvor: autor.

Ovakvi nalazi sugeriraju da sudionici istraživanja sigurnost primarno povezuju s imovinskim i podatkovnim aspektima, dok fizička sigurnost zaposlenika zauzima sporedno mjesto u percepciji rizika. To može upućivati na dominantnu orijentaciju poduzeća prema zaštiti resursa koji su izravno povezani s poslovnim procesima i zakonskim obvezama (npr. zaštita osobnih podataka), dok sigurnost ljudi, iako ključna stvar, možda nije jednako naglašena u strategijama upravljanja rizicima ili nije percipirana kao neposredna prijetnja u svakodnevnom poslovanju.

4.3. Analiza čestica namijenjenih mjerenju bihevioralnog vanjskog čimbenika

Analizom bihevioralnih vanjskih čimbenika, okviru analize čestica konstruiranih za mjerenje percepcije pritiska nadređenih, rezultati pokazuju kako su svi ispitanici odgovarali na ljestvici od 1 do 5, pri čemu su srednje vrijednosti (M) varirale od 3.12 do 4.14, što sugerira umjerenu do visoku razinu slaganja s tvrdnjama. Standardne devijacije (SD) su relativno visoke, što sugerira određenu raznolikost u odgovorima među ispitanicima. Svi rezultati Kolmogorov-Smirnov testa (K-S test) pokazali su statistički značajna odstupanja od normalne distribucije ($p < .001$). To znači da distribucije odgovora na sve četiri tvrdnje ne prate normalnu krivulju, što treba uzeti u obzir kod daljnjih statističkih analiza (npr. odabira neparametrijskih testova).

Utvrđeno je kako čestica Q16 pokazuje negativne korelacije s ostalim česticama unutar iste dimenzije. Slijedom toga, navedena je čestica za potrebe daljnjih statističkih obrada bodovana obrnuto. Deskriptivni statistički pokazatelji te čestice, zajedno s rezultatima za ostale čestice unutar iste dimenzije, prikazani su u [Tablici 8](#). Distribucije rezultata značajno odstupaju od normalne distribucije i pokazuju asimetriju nagnutu prema višim vrijednostima. Tvrdnja "Upravljanje sigurnosnim rizicima nepotrebno je nametnuto..." ima srednju vrijednost od 3.78, što upućuje na to da se ispitanici u prosjeku ne slažu s tvrdnjom (budući da je čestica obrnutog predznaka), odnosno ne smatraju upravljanje rizicima nametnutim, već ga vjerojatno vide kao opravdano. Tvrdnja o vlastitoj odgovornosti prema nadležnima ima srednju vrijednost 3.70, što pokazuje da većina ispitanika prepoznaje svoju odgovornost u području upravljanja sigurnosnim rizicima. Tvrdnja o nadzoru nad implementacijom propisa ima najnižu srednju vrijednost (3.12), što može značiti da ispitanici nisu u potpunosti uvjereni da se nadzor provodi redovito ili dosljedno. Tvrdnja da nepoštivanje propisa može imati negativne posljedice ima najvišu prosječnu vrijednost (4.14), što jasno pokazuje da ispitanici uočavaju ozbiljne posljedice kršenja sigurnosnih propisa, i za sebe i za poduzeće.

Tablica 8.*Pritisak nadređenih - deskriptivna analiza.*

Čestica	min	max	M	SD	K-S test	
					z	p
Q16	1	5	3.78	1.38	0.29	< .001
Q17	1	5	3.70	1.19	0.24	< .001
Q18	1	5	3.12	1.55	0.22	< .001
Q19	1	5	4.14	1.04	0.27	< .001

Izvor: autor.

Rezultati deskriptivne analize čestica koje ispituju utjecaj radne okoline (Tablica 9.) na stavove ispitanika o tome koliko radna okolina, uključujući kolege, interne prakse i organizacijsku kulturu, utječe na njihovo ponašanje i stavove u kontekstu upravljanja sigurnosnim rizicima. Rezultati pokazuju da ispitanici u prosjeku ocjenjuju da njihovi kolege, suradnici i partneri imaju umjereno do izrazito pozitivan odnos prema poštivanju sigurnosnih procedura. Navedeni rezultati u skladu su s teorijom planiranog ponašanja koja govori kako se subjektivne norme odnose na percipirani društveni pritisak, odnosno uvjerenja pojedinca o tome što važni referentni akteri, poput kolega, nadređenih ili bliskih osoba, očekuju od zaposlenika u vezi s ponašanjem, kao i na njegovu motivaciju da se tim očekivanjima prilagodi. Vrijednosti čestica kreću se od 3.27 do 3.62, što upućuje na relativno dobru percepciju sigurnosne kulture unutar organizacije. Čestica o razumijevanju i poštivanju sigurnosnih procedura od strane kolega imala je srednju vrijednost 3.27 (SD = 1.28), što indicira umjereni stupanj slaganja, ali i nešto veću varijabilnost u odgovorima, odnosno da nisu svi jednako uvjereni u dosljedno poštivanje pravila među kolegama. Slično, tvrdnja da većina zaposlenika poštuje propisane procedure ima srednju vrijednost 3.29 (SD = 1.21), što potvrđuje da je percepcija pravilnog ponašanja među zaposlenicima uglavnom pozitivna, ali postoje i odstupanja. Ispitanici također smatraju da zaposlenici imaju pozitivan stav prema sigurnosnim procedurama (M = 3.38; SD = 1.24), što je važan pokazatelj prihvaćanja i spremnosti za suradnju u području sigurnosti. Najviša srednja vrijednost (M = 3.62; SD = 1.16) zabilježena je kod percepcije o konkurentskim poduzećima i njihovoj implementaciji sigurnosnih propisa, što može odražavati dojam o industrijskim standardima ili pritisku konkurencije kao poticaju za vlastitu usklađenost. Rezultati Kolmogorov-Smirnov testa (K-S test) za sve čestice ukazuju na statistički značajna odstupanja od normalne distribucije ($p < .001$). Ovo sugerira da su odgovori nagnuti ili imaju asimetričnu raspodjelu, što treba imati na umu prilikom daljnjih statističkih analiza.

Tablica 9.*Radna okolina - deskriptivna analiza.*

Čestica	min	max	M	SD	K-S test	
					z	p
Q20	1	5	3.27	1.28	0.28	< .001
Q21	1	5	3.29	1.21	0.27	< .001
Q22	1	5	3.38	1.24	0.25	< .001
Q23	1	5	3.62	1.16	0.21	< .001

Izvor: autor.

4.4. Međusobne korelacije istraživanih čimbenika

Rezultati korelacijske analize (Tablica 10.) otkrivaju snažnu međusobnu povezanost između gotovo svih analiziranih dimenzija koje čine okosnicu sigurnosne kulture u organizacijama. Prihvaćenost međunarodnog standarda ISO 31000:2018 pokazala je vrlo visoku pozitivnu korelaciju s unutarnjim bihevioralnim čimbenicima ($r = .85$), sigurnosnom svjesnošću ($r = .84$), percipiranom učinkovitošću sigurnosnih mjera ($r = .89$), vanjskim bihevioralnim čimbenicima ($r = .91$) te utjecajem radne okoline ($r = .87$). Ovakvi rezultati sugeriraju da je implementacija standarda u velikoj mjeri povezana s pozitivnim sigurnosnim ponašanjima, stavovima i percepcijama zaposlenika, kao i s općom podrškom iz okruženja, što je u skladu s postavkama teorije planiranog ponašanja.

Bihevioralni unutarnji čimbenici, koji uključuju osobnu odgovornost, proaktivnost i angažman u sigurnosnim pitanjima, pokazuju izrazito jake pozitivne korelacije sa sigurnosnom svjesnošću ($r = .89$) i percepcijom učinkovitosti ($r = .85$). To upućuje na to da zaposlenici koji su unutarnje motivirani i svjesni svoje uloge u sustavu sigurnosti ujedno procjenjuju sigurnosne mjere kao učinkovitije, te iskazuju višu razinu općeg znanja i uključenosti. Sličan obrazac odnosa uočen je i kod vanjskih bihevioralnih čimbenika, koji su snažno korelirani s gotovo svim pozitivnim dimenzijama, što dodatno potvrđuje važnost poticajnog socijalnog i organizacijskog okruženja.

Za razliku od navedenih dimenzija, percipirani pritisak nadležnih tijela pokazuje izrazito negativne korelacije sa svim drugim varijablama, od ISO standarda ($r = -.83$) do vanjskih bihevioralnih utjecaja ($r = -.94$) i sigurnosne svjesnosti ($r = -.77$). Takvi rezultati upućuju na to da zaposlenici koji osjećaju jak pritisak od strane nadležnih institucija ili regulatornih tijela istovremeno iskazuju niži stupanj unutarnje motivacije, slabije prihvaćaju sigurnosne standarde i imaju nižu percepciju učinkovitosti sustava. Drugim riječima, percipirani pritisak može djelovati kontraproduktivno potičući formalnu usklađenost, ali narušavajući autonomiju, povjerenje i spremnost na proaktivno ponašanje. Dodatno, rezultati ukazuju na značajnu ulogu radne okoline, koja pozitivno korelira s većinom mjera sigurnosne kulture, a negativno s percipiranim pritiskom nadležnih ($r = -.77$). To pokazuje da uključivo radno okruženje koje podržava radnu okolinu može ublažiti negativne učinke vanjskog pritiska, naglašavajući važnost organizacijske klime kao zaštitnog faktora.

Tablica 10.

Međuodnos prihvaćenosti ISO 31000:2018 i bihevioralnih unutarnjih i vanjskih čimbenika.

Varijabla	ISO	BUČ	SS	PU	PI	BVČ	PN	URO
ISO	-							
BUČ	.85	-						
SS	.84	.89	-					
PU	.89	.85	.81	-				
PI	.53	.82	.52	.52	-			
BVČ	.91	.85	.85	.85	.57	-		
PN	-.83	-.80	-.77	-.80	-.54	-.94	-	
URO	.87	.80	.82	.80	.51	.94	-.77	-

Izvor: autor.

Rezultati provedene analize ukazuju na izrazitu međusobnu povezanost ključnih dimenzija sigurnosne kulture i sustava upravljanja sigurnosnim rizicima na organizacijskoj razini. Visoke pozitivne korelacije između prihvaćenosti ISO 31000:2018 i varijabli poput

sigurnosne svjesnosti, percepcije učinkovitosti i bihevioralnih čimbenika jasno upućuju na to da standardi upravljanja rizicima mogu djelovati kao temeljna osnova za razvoj integritetnog, proaktivnog i održivog pristupa organizacijskoj sigurnosti.

Posebno je značajna uloga unutarnjih i vanjskih bihevioralnih čimbenika, koji pokazuju snažnu povezanost sa svim pozitivnim aspektima sigurnosnog ponašanja i stavova. Ovi rezultati potvrđuju teorijska polazišta koja naglašavaju važnost unutarnje motivacije, stavova zaposlenika i socijalne dinamike radne sredine kao ključnih faktora u implementaciji sigurnosnih politika. Također, snažna povezanost radne okoline sa sigurnosnom svjesnošću i percepcijom učinkovitosti upućuje na važnost kulture povjerenja, suradnje i kolektivne odgovornosti u smanjenju organizacijskog rizika.

Suprotno tome, percipirani pritisak od strane nadležnih institucija negativno je povezan sa svim ostalim varijablama. Ova pojava sugerira da regulatorni zahtjevi, ako su percipirani kao vanjski i nametnuti, mogu umanjiti unutarnju motivaciju, oslabiti prihvaćenost standarda i narušiti doživljaj učinkovitosti sigurnosnih mjera. Ovi rezultati podupiru suvremena istraživanja koja ističu kako sigurnosna usklađenost ne proizlazi isključivo iz kontrole i nadzora, već prvenstveno iz razumijevanja, uključivanja i kulturne integracije sigurnosnih vrijednosti. Dodatno, visoka razina sigurnosne svjesnosti i percepcije učinkovitosti među ispitanicima upućuje na snažnu orijentaciju zaposlenika prema sigurnosti, unatoč ograničenoj učestalosti stručnih edukacija. Ovaj nesrazmjer može ukazivati na važnost svakodnevnih iskustava, neformalnog učenja i organizacijskog modeliranja ponašanja, što bi trebalo dodatno istražiti u budućim istraživanjima.

4.5. Ograničenja i buduća istraživanja

Istraživanje je provedeno u Hrvatskoj na uzorku od 125 ispitanika prema posebnim kriterijima, stoga se dobiveni rezultati ne mogu u potpunosti generalizirati izvan hrvatskog konteksta, s obzirom na moguće kulturne i socioekonomske razlike među zemljama. Buduća istraživanja trebala bi uključiti longitudinalne pristupe i proširiti analizu na različite sektore i organizacijske kontekste kako bi se dodatno istražila uloga bihevioralnih čimbenika u procesima prihvaćanja sigurnosnih normi. Osobito bi korisno bilo istražiti i organizacijske mehanizme koji ublažavaju negativne učinke regulatornog pritiska te ojačati teorijsku i praktičnu integraciju između sigurnosne kulture i sustava upravljanja rizicima.

5. Zaključak

Dobiveni rezultati pružaju relevantne spoznaje u način na koji se različiti čimbenici međusobno isprepliću u oblikovanju organizacijskog odgovora na sigurnosne izazove. Ključni zaključak proizlazi iz činjenice da učinkovito upravljanje sigurnosnim rizicima nije isključivo tehničko pitanje implementacije normi, već kompleksna interakcija standarda, ponašanja, radne okoline i regulatornog konteksta.

Testiranjem hipoteza potvrđeno je da i vanjski i unutarnji bihevioralni čimbenici imaju statistički značajan utjecaj na prihvaćenost ovog standarda, pri čemu se jasno ističe uloga radne okoline, sigurnosne svijesti i percepcije učinkovitosti upravljanja sigurnosnim rizicima. Posebno je izražena pozitivna korelacija između radne okoline i prihvaćenosti ISO standarda, što u skladu s teorijom planiranog ponašanja upućuje na to da poticajno, suradničko i sigurnosno osviješteno okruženje olakšava integraciju formalnih normi u organizacijsku praksu. Suprotno tome, rezultati su također potvrdili kako pritisak nadređenih korelira negativno s prihvaćanjem norme. Ova negativna povezanost upućuje na to da percipirani vanjski pritisci mogu izazvati otpor, smanjiti unutarnju motivaciju i oslabiti stvarnu integraciju sigurnosnih načela. Unutarnji bihevioralni čimbenici također imaju značajan utjecaj na prihvaćenost standarda. Dobiveni rezultati snažno podupiru važnost znanja, razumijevanja i osobne identifikacije sa sigurnosnim načelima i pokazuju kako su zaposlenici koji percipiraju sigurnosne mjere kao učinkovite, skloniji prihvaćanju i provođenju normi,

dok percepcija izloženosti djeluje kao dodatni, ali ne presudan poticaj za usvajanje standardiziranih pristupa rizicima.

Rezultati potvrđuju da prihvaćenost norme ISO 31000:2018 nije isključivo rezultat formalnog zahtjeva ili institucionalnog pritiska, već kompleksan proces oblikovan interakcijom individualnih uvjerenja, kolektivne radne klime i načina na koji zaposlenici percipiraju korisnost sigurnosnih mjera. U tom kontekstu, implementacija standarda mora biti praćena strateškim upravljanjem ljudskim faktorom - edukacijom, poticanjem unutarnje motivacije i jačanjem organizacijske kulture koja razumije, prihvaća i dosljedno primjenjuje sigurnosne norme.

Za organizacije koje žele razviti održiv i učinkovit sigurnosni sustav, ključno je ulagati ne samo u usklađenost s propisima, već i u jačanje unutarnje motivacije zaposlenika, promicanje pozitivne sigurnosne kulture te poticanje suradnje između svih dionika. Također, odnos s nadzornim tijelima treba biti temeljen na partnerstvu, a ne na pritisku, kako bi se izbjeglo smanjenje autonomije i otpora prema promjenama. Preporučuje se usmjeriti se na unutarnju motivaciju zaposlenika kroz uključivanje, osnaživanje i kontinuiranu edukaciju, umjesto oslanjanja isključivo na vanjske zahtjeve i formalne mehanizme nadzora. Nadalje, sustavnom implementacijom ISO 31000 u skladu s organizacijskom kulturom i specifičnostima sektora, pri čemu standard ne bi trebao biti samo formalni okvir, ova norma postala bi alat za jačanje sigurnosne svijesti i integraciju upravljanja rizicima u svakodnevne procese. Predlaže se također ulaganje u izgradnju pozitivne radne okoline koja potiče otvorenu komunikaciju, timsku suradnju i uzajamnu odgovornost za sigurnost, jer takvo okruženje dodatno povećava učinkovitost sigurnosnih politika. Ono iziskuje i preoblikovanje načina na koji se komunicira regulatorni nadzor umjesto percipiranog „nametanja“ od strane nadležnih institucija, kao i razvoj partnerskog odnosa koji podržava organizacije u izgradnji kapaciteta i usklađivanju s propisima.

The article is relevant to UN Sustainable Development Goals:



Literatura

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management*, 1(2), 104–114. <https://doi.org/10.1515/dim-2017-0006>
- Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 15)*, 103–122. USENIX Association, USA.
<https://web.archive.org/web/20170802213747/https://www.usenix.org/conference/soups2015/proceedings/presentation/blythe>
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151–164.
<https://doi.org/10.1057/ejis.2009.8>
- Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. In L. Little, E. Sillence, & A. Joinson (Eds.), *Behavior change research and theory: Psychological and technological perspectives*, 115–136. Elsevier Academic Press. <https://doi.org/10.1016/B978-0-12-802690-8.00004-9>

- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Chongrui, L., Wang, C., Wang, H., & Niu, B. (2020). Influencing factors of employees' information systems security policy compliance: An empirical research in China. *E3S Web of Conferences*, 218, 04032. <https://doi.org/10.1051/e3sconf/202021804032>
- Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), 525–554. <https://doi.org/10.25300/MISQ/2019/15117>
- Giovanetti, E., Righi, E., Lauriola, P., Ghinoi, A., & Soldati, M. (2021). Disaster risk reduction and interdisciplinary education and training. *Progress in Disaster Science*, 10, 100165. <https://doi.org/10.1016/j.pdisas.2021.100165>
- Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2017). Correlating human traits and cybersecurity behavior intentions. *Computers & Security*, 73, 345–358. <https://doi.org/10.1016/j.cose.2017.11.015>
- Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165. <https://doi.org/10.1016/j.dss.2009.02.005>
- Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- Kaymaz, K. (2020). The analysis of the relations among normative beliefs, self-efficacy, and intention to comply within the frame of information security policies. *The Journal of Industrial Relations & Human Resources*, 22(1), 1–20. Retrieved from: <https://www.isguc.org/download.php?id=738&tk=327554bce8b05e8d14b072b4e650af67&f=738.pdf&user=&lg=tr>
- Koohang, A., Anderson, J., Nord, J. H., & Paliszkievicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, 120(2), 231–247. <https://doi.org/10.1108/IMDS-07-2019-0412>
- Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management*, 14(4), 272–300. <https://doi.org/10.1057/rm.2012.9>
- Lounsbury, M., & Wang, M. S. (2020). Into the clearing: Back to the future of constitutive institutional analysis. *Organization Theory*, 1(1). <https://doi.org/10.1177/2631787719891173>
- Merhi, M., & Ahulwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, 92, 37–46. <https://doi.org/10.1016/j.chb.2018.10.031>
- Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play? *International Journal of Project Management*, 34(8), 1568–1578. <https://doi.org/10.1016/j.ijproman.2016.08.002>
- Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security behavior: An Australian web-based study. *Lecture Notes in Computer Science*, 9190, 231–241. https://doi.org/10.1007/978-3-319-20376-8_21
- Pokrajčić, I. (2025). *Determinants of the security risk management in middle and large companies in the segment of the national critical infrastructure of the Republic of Croatia in accordance to ISO 31000:2018*. [Doctoral dissertation, University of Zagreb]. <https://urn.nsk.hr/urn:nbn:hr:148:222681>
- Pokrajčić, I., & Lazibat, T. (2025). The correlation between the implementation of ISO 31000:2018 and the maturity of security risk management in companies from the national critical infrastructure sector of the Republic of Croatia. *Ekonomika i Praksa*, 34(2), 369–394. <https://doi.org/10.17818/EMIP/2025/26>
- Scolobig, A., Prior, T., Schröter, D., Jörin, J., & Patt, T. (2015). Towards people-centred approaches for effective disaster risk management: Balancing rhetoric with reality. *International Journal of Disaster Risk Reduction*, 12, 202–212. <https://doi.org/10.1016/j.ijdrr.2015.01.006>

- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487–502. <https://doi.org/10.2307/25750688>
- Sommestad, T., Karlzén, H., Nilsson, P., & Hallberg, J. (2016). An empirical test of the perceived relationship between risk and the constituents severity and probability. *Information and Computer Security*, 24(2), 194–204. <https://doi.org/10.1108/ICS-01-2016-0004>
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276. <https://doi.org/10.1287/isre.1.3.255>
- Talib, F., & Siddique, J. (2015). Identification of total quality management enablers and information technology resources for ICT industry: A Pareto analysis approach. *International Journal of Information Quality*, 4(1), 18–41. <https://doi.org/10.1504/IJIQ.2015.071675>
- Warrington, C., Syed, J., & Tappin, R. (2021). Personality and employees' information security behavior among generational cohorts. *Computer and Information Science*, 14(1), 26–36. <https://doi.org/10.33423/jop.v22i3.5647>

Behavioral Approach to Security Risk Management: Empirical Research Results

ABSTRACT

Purpose: In the context of the growing interest in integrating psychological and social dimensions of risk management, the aim of this article is to analyze the correlation between behavioral factors and the acceptance of the ISO 31000:2018 standard. **Design/Methodology:** The theoretical framework is based on the Theory of Planned Behavior (TPB), taking into account the influence of attitudes, subjective norms, and perceived behavioral control on employees' safety-oriented behavior. The empirical research was conducted on a sample of 125 respondents, examining external factors (pressure of superiors, work environment) and internal factors (security awareness, perceived effectiveness, and risk exposure) in relation to the acceptance of the standard. **Findings:** The results indicate a statistically significant positive correlation between the influence of the work environment and the acceptance of the standard, whereas pressure of superiors demonstrated a negative correlation, suggesting employees' resistance to an authoritarian approach. The findings further confirm the importance of security culture and a positive organizational climate in promoting compliance with security standards. **Practical implications:** The obtained results provide an empirical basis for redefining organizational risk management strategies through the integration of behavioral insights into institutional frameworks, with the aim of enhancing the efficiency and sustainability of security management systems. **Originality/value:** This study contributes to the literature by providing empirical evidence on the role of behavioral factors in the process of adopting the ISO 31000:2018 standard, emphasizing the need to incorporate behavioral aspects into the development of organizational security culture and contemporary security risk management practices.

Keywords: risk management, security risks, behavioral analysis, ISO 31000:2018